(36)

PATENT ABSTRACTS OF JAPAN

(11)Publication number :	2003-317376
(43)Date of publication of application :	07.11.2003

(51)Int.Cl.	G11B 20/10 G06F 12/14 G06F 15/00 H04N 7/173

(21)Application number :	2002-111555	(71)Applicant :	SONY CORP
(22)Date of filing :	15.04.2002	(72)Inventor :	KAWAMOTO HIROSHI ISHIGURO RYUJI EOMO YUICHI NAGANO MOTOHIKO

(54) INFORMATION MANAGEMENT APPARATUS AND METHODRECORDING MEDIUMAND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent contents from being illegally utilized.

SOLUTION: Contents recorded on a CD 81 are captured by a ripping module 91 of a client 1 and saved in a storage part 28. In the client 1a contents ID (CID) for identifying contents and a unique ID (Uniq ID) intrinsic for the client 1 (ripping module 91) are generated and the IDs are added to the contents captured by the ripping module 91. Besidesin the client 1a right to use in which use conditions of contents or the like is described is generated and saved. In the right to use is described information representing that the reproduction of contents is permitted only in a device (client) having the same ID as the unique ID added to the contents. This invention can be applied to an information processor such as a personal computer.

CLAIMS

[Claim(s)]

[Claim 1]An information management device which manages contentscomprising:

A contents acquisition means which acquires said contents.

An identification information acquisition means which acquires identification

information which identifies said information management device.
A content storing means which adds and memorizes said identification information acquired by said identification information acquisition means to said contents acquired by said contents acquisition means.
As information about use of said contentsit is said identification information.
A right-of-use memory measure which memorizes the right of use in which said identification information added to said contents and information to which use with the equipment with which the same identification information is acquired is permitted are included.

[Claim 2]The information management device according to claim 1 having further a reproduction means which reproduces said contents when said identification information added to said contents and said identification information acquired by said identification information acquisition means are the same.
[Claim 3]The information management device according to claim 1wherein said contents acquisition means acquires said contents from a predetermined recording medium with which said information management device was equipped.
[Claim 4]The information management device according to claim 1wherein said identification information acquisition means makes a generated random number said identification information.
[Claim 5]A contents acquisition step which acquires said contents in an information management method of an information management device which manages contentsAn identification information acquisition step which acquires identification information which identifies said information management deviceA contents memory step which adds and memorizes said identification information acquired by processing of said identification information acquisition step to said contents acquired by processing of said contents acquisition stepAn information management method containing a right-of-use memory step which memorizes the right of use in which information to which use with the equipment with which the identification information same as information about use of said contents as said identification information and said identification information added to said contents is set up is permitted is included.
[Claim 6]A contents acquisition control step which controls acquisition of said contents in a recording medium of an information management device which manages contentsAn identification information acquisition control step which controls acquisition of identification information which identifies said information management deviceA contents storage control step which controls memory performed to said contents acquired by processing of said contents acquisition control step by adding said identification information acquired by processing of said identification information acquisition control stepAs information about use of said contentssaid identification informationA recording medium with which a program which a computer containing a right-of-use storage control step which controls memory of the right of use in which information to which use with the equipment with which the same identification information as said identification

information added to said contents is set up is permitted is included can read is recorded.
[Claim 7]A program which performs a right-of-use storage control step which controls memory of the right of usecomprising:
A contents acquisition control step which controls acquisition of said contents to a computer which controls an information management device which manages contents.
An identification information acquisition control step which controls acquisition of identification information which identifies said information management device.
A contents storage control step which controls memory performed to said contents acquired by processing of said contents acquisition control step by adding said identification information acquired by processing of said identification information acquisition control step.
Information to which use with the equipment with which the identification information same as information about use of said contents as said identification information and said identification information added to said contents is set up is permitted.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the information management device which enables it to prevent unjust reproduction of contents easily especially and a methoda recording mediumand a program about an information management device and a methoda recording mediumand a program.
[0002]
[Description of the Prior Art]In recent yearsvarious kinds of broadband environment is being improved and the distribution service of various kinds of contentssuch as music data and a video datais beginning to be started completely.
[0003]For examplein [subscribed type (subscription type) music distribution service of "PressPlay (trademark)" etc. is performedand] this music distribution serviceWithin the limits of the conditions which a user is paying the charge of a monthly fixed amountand are set up beforehand. for examplethe case of streaming reproduction -- up to 1000 music -- refreshable and the case where download and it saves at the hard disk of a personal computer -- up to 100 music -- the preservation possibility of. When [to CD(Compact Disk)-R] writing in (copy)a music content can be used within the limits of which conditions that can be copied to 20 music.
[0004]By the wayfor example as a system which manages the right information data of the user who receives offer of the contents by such distribution service to JPH2001-352321A. In the system which arranges the node corresponding to two

or more services to tree formFrom the node corresponding to predetermined service. Validation key blocks (EKB (Enabling Key Block)) including the key information (DNK (Device Node Key)) set as the node which exists on the path to the node (device) of each leaf belonging to the service. Using is indicated.
[0005]In this systemEKB is added to the contents distributed in a certain serviceand the device which permits use of service is managed by making the updated key information which is included in EKB acquire using DNK given to each device. In this casethe device which cannot acquire the updated key information from EKB cannot receive offer of service after that using DNK.
[0006]And it enables it to manage use of the contents in each devicewithout this performing authenticating processing etc. each time between the server and device which provide contents.
[0007]In the system by which it does in this way and the right information data of contents are managedFor examplethe device which imported contents from CD (Compact Disk) is made as [manage / by ICV (Integrity Check Value) / the contents].
[0008]Drawing 1 is a figure showing the composition which manages the imported contents by ICV typically.
[0009]As shown in drawing 1for exampledevicessuch as a personal computerThe contents (music data) imported from CD are registered into the management table of a hard diskMAC (Message Authentication Code) (C1C2--Cn) generated based on the contents registered is applied to ICV=hash (KicvC1C2--Cn)and ICV is generated. Kicv is the key information for generating ICV.
[0010]And if it generates to a contents generate timeICV saved safely is compared with ICV newly generated to the predetermined timing at the time of reproductionetc. and the same ICV is obtainedIt is judged with there having been no alteration in contentsand when obtained ICV differs from the thing of a contents generate time on the other handit is judged with contents having had an alteration. After the case where it is judged with there having been no alteration in contentsregeneration of contents is performedand when judged with there having been an alterationregeneration is not performed. Thereforetherebyreproduction of the altered contents is prevented.
[0011]
[Problem to be solved by the invention]Howeverwhen managing contents by ICV as mentioned abovewhenever it imports contentsor whenever it reproduced contentsICV had to be generatedand SUBJECT that the processing burden was large occurred.
[0012]Thereforefor portable devicessuch as a device for music reproductionwhen the highly efficient operation part in which the hash operation for generating ICV is possible is needed and such operation part is providedthe cost of a device will go up as a result.
[0013]This invention is made in view of such a situationand enables it to prevent unjust reproduction of contents easily.
[0014]

[Means for solving problem]This invention is characterized by an information management device comprising the following.
The contents acquisition means which acquires contents.
The identification information acquisition means which acquires the identification information which identifies an information management device.
The content storing means which adds and memorizes the identification information acquired by the identification information acquisition means to the contents acquired by the contents acquisition means.
The right-of-use memory measure which memorizes the right of use in which identification informationthe identification information added to contentsand the information to which use with the equipment with which the same identification information is acquired is permitted are included as information about use of contents.

[0015]The reproduction means which reproduces contents is established furtherand it may be made to reproduce contents only when the identification information by which the reproduction means is added to contentsand the identification information acquired by the identification information acquisition means are the same.
[0016]A contents acquisition means acquires contents from the predetermined recording medium with which the information management device was equipped.
[0017]It may be made to add an identification information acquisition means to contents etc. by making into identification information the random number which he generated. Identification information may be provided from external equipment etc.
[0018]This invention is characterized by the information management method of an information management device comprising the following.
The contents acquisition step which acquires contents.
The identification information acquisition step which acquires the identification information which identifies an information management device.
The contents memory step which adds and memorizes the identification information acquired by processing of the identification information acquisition step to the contents acquired by processing of the contents acquisition step.
The right-of-use memory step which memorizes the right of use in which the information to which use with the equipment with which the identification information same as information about use of contents as identification information and the identification information added to contents is set up is permitted is included.

[0019]A contents acquisition control step which controls acquisition of contents in a recording medium of an information management device of this inventionAn identification information acquisition control step which controls acquisition of identification information which identifies an information management deviceA contents storage control step which controls memory performed to contents

acquired by processing of a contents acquisition control step by adding identification information acquired by processing of an identification information acquisition control stepA right-of-use storage control step which controls memory of the right of use in which information to which use with the equipment with which the identification information same as information about use of contents as identification information and identification information added to contents is set up is permitted is includedA program which a computer is made to execute is recorded.

[0020]A contents acquisition control step which controls acquisition of contents to a computer by which a program of this invention controls an information management device which manages contentsAn identification information acquisition control step which controls acquisition of identification information which identifies an information management deviceA contents storage control step which controls memory performed to contents acquired by processing of a contents acquisition control step by adding identification information acquired by processing of an identification information acquisition control stepA right-of-use storage control step which controls memory of right-of-use information in which information to which use with the equipment with which the identification information same as information about use of contents as identification information and identification information added to contents is set up is permitted is included is performed.

[0021]In the information management device of this inventiona methodand a programcontents are acquired and the identification information which identifies an information management device is acquired. The acquired identification information is added and memorized to the acquired contentsand as information about use of contentsThe right of use in which identification informationthe identification information added to contentsand the information to which use with the equipment with which the same identification information is acquired is permitted are included is memorized.

[0022]

[Mode for carrying out the invention]Drawing 2 shows the composition of the contents providing system which applied this invention. Client 1-11-2 (hereafterwhen these clients do not need to be distinguished separatelythe client 1 is only called) is connected to the Internet 2. In this examplealthough two clients are shownthe client of the arbitrary number is connected to the Internet 2.

[0023]On the Internet 2. When the content server 3 which provides contents to the client 1the license server 4 which gives the right of use required to use the contents which the content server 3 provides to the client 1and the client 1 receive the right of useThe fee collection server 5 which performs accounting to the client 1 is connected.

[0024]Only the number also with arbitrary these content servers 3license server 4and fee collection server 5 is connected to the Internet 2.

[0025]Drawing 3 expresses the composition of the client 1.

[0026]In drawing 3CPU(Central Processing Unit) 21Various kinds of processings

are performed according to the program memorized by ROM(Read Only Memory) 22 or the program loaded to RAM(Random Access Memory) 23 from the storage parts store 28. the timer 20 -- a time check -- it operates and time information is supplied to CPU21. To RAM23CPU21 performs various kinds of processings againand also required data etc. are memorized suitably.

[0027]The encryption decoding part 24 performs processing which decodes the already enciphered contents while enciphering contents. For examplethe codec part 25 encodes contents by ATRAC(Adaptive Transform Acoustic Coding)3 system etc.and is made to supply and record them on the semiconductor memory 44 connected to the drive 30 via the input/output interface 32. Or the codec part 25 decodes the data which was read from the semiconductor memory 44 via the drive 30 and which is encoded again. The semiconductor memory 44 is constituted by the memory stick (trademark) etc.for example.

[0028]CPU21ROM22RAM23the encryption decoding part 24and the codec part 25 are mutually connected via the bus 31. The input/output interface 32 is also connected to this bus 31 again.

[0029]The input part 26CRT (Cathode Ray Tube) which become the input/output interface 32 from a keyboarda mouseetc.The communications department 29 which comprises the storage parts store 28a modema terminal adopteretc. which comprise the outputting part 27 which consists of a display which consists of LCD (Liquid Crystal Display) etc.a loudspeakeretc.a hard disketc. is connected. The communications department 29 performs the communications processing through the Internet 2. The communications department 29 performs the communications processing of an analog signal or a digital signal among other clients again.

[0030]The drive 30 is connected to the input/output interface 32 again if neededIt is suitably equipped with the magnetic disk 41the optical disc 42the magneto-optical disc 43or the semiconductor memory 44and the computer program read from them is installed in the storage parts store 28 if needed.

[0031]Although a graphic display is omittedthe content server 3the license server 4and the fee collection server 5 are also constituted by the client 1 shown in drawing 3and the computer which has the same composition fundamentally. Thenin the following explanationthe composition of drawing 3 is quoted also as composition of the content server 3the license server 4the fee collection server 5etc.

[0032]In this inventionas shown in drawing 4a device and a key are managed based on the principle of a broadcasting yne KURIPUSHON (Broadcast Encryption) system. A key is made into a class tree structure and is equivalent to a key with leaf (leaf) of the bottom peculiar to each device. The class tree structure lock management used for the system of this invention is indicated to JP2001-352321A. In the case of the example of drawing 4the key corresponding to 16 devices from the number 0 to the number 15 is generated.

[0033]Each key is specified corresponding to each node of the tree structure shown by a figure Nakamaru seal. Corresponding to the root node of the highest rungthe route key KR (it is also suitably called Kroot) is prescribed by this

exampleand the key K0 and K1 are prescribed corresponding to the 2nd step of node. Corresponding to the 3rd step of nodethe keys K00 thru/or K11 are specifiedand the key K000 thru/or the key K111 are specified corresponding to the node of the 4th step. And the keys K0000 thru/or K1111 support the leaf (device node) as a node of the bottomrespectively.

[0034]Since it is considered as the layered structurethe key of the higher rank of the key K0010 and the key K0011 is set to K001and the key of the higher rank of the key K000 and the key K001 is set to K00for example. Hereaftersimilarlythe key of the higher rank of the key K00 and the key K01 is set to K0and the key of the higher rank of the key K0 and the key K1 is set to KR.

[0035]The key using contents is managed by the key corresponding to each node of one path from the device node (leaf) of the bottom to the root node of the highest rung. For examplein the device corresponding to the leaf of the number 3the key for using contents is managed by each key of the path containing the key K0011K001K00K0and KR.

[0036]In the system of this inventionas shown in drawing 5it is a keying system constituted based on the principle of drawing 4and management of the key of a device and the key of contents is performed. In the example of drawing 58+24+32 steps of nodes are made into a tree structureand a category corresponds to each node from a root node to eight steps of a low rank. The category in here means categoriessuch as a category of the apparatus which uses semiconductor memorysuch as a memory stickfor exampleor a category of apparatus which receives digital broadcasting. And this system (T system is called suitably) corresponds to one node in this category node as a system which manages the right of use.

[0037]That isthe service which a service provider or a service provider provides corresponds by the key corresponding to 24 steps of a younger class's nodes further from the node of T system. Thereforein the example of drawing 5the service provider of 2^{24} (about 16 mega) or service can be specified. 32 steps of classes of the bottom can prescribe the user (client 1) of 2^{32} (about 4 giga). The key corresponding to each node on the path from 32 steps of nodes of the bottom to the node of T system constitutes DNK (Device Node Key)and ID corresponding to the leaf of the bottom is set to leaf ID.

[0038]The contents key which enciphered contents is enciphered by updated route key KR'and the updating node key of the class of a higher rankIt is enciphered using the updating node key of the class of the latest low rankand is arranged in EKB (Enabling Key Block: validation key blocks) (with reference to drawing 7it mentions later).

[0039]The updating node key of the stage on one is enciphered from the end in EKB by the node key or leaf key of an end of EKBand it is arranged in EKB. One key of the DNK(s) described by service information is used for the client 1Using the node key which decoded the updating node key of the class of the latest higher rank described by EKB distributedand decoded and obtained it with contentsit is described by EKB and also the updating node key of the class on it is

decoded. By performing same processing one by onethe client 1 can obtain updating route key KR'. Service information is supplied from the license server 4when the information about the client 1 is registeredand it calls a license the combination of the right of use which are this service information and the information which are mentioned laterand to which use of specific contents is permitted.

[0040]Drawing 6 is a figure showing the concrete example of a classification of the category of a class tree structure.

[0041]In drawing 6route key KR2301 is set to the highest rung of a class tree structurethe node key 2302 is set to the following intermediate stagesand the leaf key 2303 is set to the bottom. Each device holds a device node key (DNK) which consists of each leaf keyand a series of node keys from a leaf key to a route key and a route key.

[0042]A predetermined node of the Mth step (an example of drawing 5 M= 8) is set up as the category node 2304 from the highest rung. That islet each of a node of the Mth step be a device setting-out node of a specific category. Let M+1 or less step of nodeand a leaf be a node and a leaf about a device contained in the category by making one node of the Mth step into the peak.

[0043]For examplea category [memory stick (trademark)] is set to the one node 2305 of the Mth step of drawing 6and the node which stands in a row below in this nodeand a leaf are set up as the node or leaf only for a category containing various devices which use memo RISUTEIIKU. That is2305 or less node is defined as the related node of the device defined as the category of a memory stickand a set of a leaf.

[0044]The low-ranking stage can be set up as the subcategory node 2306 by several steps from M stage. In the example of drawing 6the node 2306 of [the vessel only for reproduction] is set up as a subcategory node contained in the category of the device which uses a memory stick for the node under two steps of the category [memory stick] node 2305. To 2306 or less node of the vessel only for reproduction which is a subcategory node. The node 2307 of the telephone with a music reproduction function included in the category of the vessel only for playback is set upand the [PHS] node 2308 contained in the low rank at the category of a telephone with a music reproduction function and the [cellular-phone] node 2309 are set up further.

[0045]A category and a subcategory only not only in the kind of devicefor example A certain makerIt is possible to set up in arbitrary units (these are generically called an entity hereafter)such as the node which a content providera settlement-of-accounts organizationetc. manage uniquelyi.e.a batcha jurisdiction unitor a providing service unit.

[0046]For exampleby setting up one category node as a peak node only for game machine machine XYZ which a game machine machine maker sellsIn the game machine machine XYZ which a maker sellsthe node key of the lower berth below the peak nodeBy being able to store and sell a leaf keyand generating and distributing after that EKB constituted by the node key below the peak node

keyand the leaf key. The message distribution processing of enciphered contentthe message distribution processing of various keysan update processetc. can be performed only to the device (game machine machine XYZ) below a peak node.

[0047]That isrenewal of a keyetc. can be performedwithout completely affecting the device belonging to the node of other categories which is not classified as a peak node.

[0048]When it is revealed in t at a certain time that the key K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose -- a node key -- K -- 001 -- K -- 00 -- K -- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of the generation (Generation) t of the key Kaaa.

[0049]distribution **** of an updating key -- it ****** just. Renewal of a key is performed by storing in a predetermined recording medium the table constituted by EKB shown in drawing 7for exampleand supplying it to the devices 01and 2 via a network. EKB is constituted by the cryptographic key for distributing the key newly updated by the device corresponding to each leaf (node of the bottom) which constitutes a tree structure as shown in drawing 4.

[0050]EKB shown in drawing 7 is constituted as block data with the data configuration which can update only the required device of renewal of a node key. In the devices 01and 2 in the tree structure shown in drawing 4the example of drawing 7 is the block data formed for the purpose of distributing the generation's t updating node key.

[0051]The devices 0 and 1 are received so that clearly from drawing 4updating -- a node key -- ****** -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- providing -- things -- required -- a device -- two -- receiving -- updating -- a node key -- ****** -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- providing -- things -- being required .

[0052]As shown in EKB of drawing 7two or more cryptographic keys are contained in EKBfor examplethe cryptographic key of the bottom of drawing 7 is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- oneself -- having -- a leaf key -- K -- 0010 -- a cryptographic key -- decoding -- updating -- a node key -- K -- (-- t --) -- 001 -- being acquirable .

[0053]using updating node key K(t)001 obtained by decodingthe device 2 can decode the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) from under drawing 7and can acquire updating node key K(t)00.

[0054]The device 2 is decoding the 2nd step of cryptographic key Enc (K (t) 00K(t)0) from on drawing 7 similarlyUpdating node key K (t) 0 can be acquired and updating route key K(t) R can be acquired from on drawing 7 using this by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R).
[0055]on the other hand -- a node key -- K -- 000 -- updating -- an object -- a key -- containing -- not having -- a node -- zero -- one -- updating -- a node key -- ****** -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is .
[0056]The nodes 0 and 1 acquire updating node key K(t)00 using the debye skiing K0000 and K0001 by decoding the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 7Similarly one by one by decoding the 2nd step of cryptographic key Enc (K (t) 00K(t)0) from on drawing 7. Updating node key K (t) 0 is acquired and updating route key K(t) R is further acquired from on drawing 7 by decoding the 1st step of cryptographic key Enc (K(t) 0 and K (t) R). Thusthe devices 01and 2 can obtain updated key K(t) R.
[0057]The index of drawing 7 shows the actual address of the node key and leaf key which are used as a decryption key for decoding the cryptographic key shown in the right-hand side of a figure.
[0058]When renewal of node key K(t) 0 and K (t) R of the upper stage of the tree structure shown in drawing 4 is unnecessary and the update process of only the node key K00 is requiredupdating node key K(t)00 can be distributed to the devices 01and 2 by using EKB of drawing 8.
[0059]EKB shown in drawing 8 is available when distributing the new contents key shared in a specific groupfor example.
[0060]For examplethe devices 012and 3 in the group to whom it is shown with the alternate long and short dash line of drawing 4 use a certain recording mediumand presuppose that it is required to set up new common contents key K(t) con to those devices. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- being new -- being common -- updating -- a contents key -- K -- (-- t --) -- con -- enciphering -- having had -- data -- Enc (K (t) 00K(t) con) -- drawing 8 -- being shown -- having -- EKB -- distributing -- having . By this distributionthe distribution as data of the device 4 etc. which other groups' apparatus cannot decode is attained.
[0061]That isthe devices 01and 2 can obtain contents key K(t) con at the t time by decoding code data using key K(t)00 which processed and obtained EKB.
[0062]Drawing 9 as an example of processing which obtains contents key K(t) con in t timeK (t) The data Enc (K (t) 00K(t) con) in which new common contents key K(t) con was enciphered by 00and EKB shown in drawing 8 are the figures showing typically processing of the device 0 provided via a predetermined recording medium. That isan example of drawing 9 is an example which set encryption message data based on EKB to contents key K(t) con.
[0063]As shown in drawing 9the device 0 generates node key K(t)00 using EKB at the generation t time stored in a recording mediumand the node key K000

currently beforehand prepared for itself by EKB processing (processing which undoes a key one by one) which was mentioned above. In order to decode updating contents key K(t) con and to use it behind using updating node key K(t)00 decodedthe device 0 is the leaf key K0000 which he hasand enciphers and stores updating contents key K(t) con.

[0064]Drawing 10 is a figure showing the example of a format of EKBand EKB which consists of such various kinds of information is contained in the header of contents data.

[0065]The version 61 is an identifier which shows the version of EKB. This version 61 has the function to identify the newest EKBand a function which shows a correspondence relation with contents. The depth 62 shows the hierarchy number of the class tree to the device of the distribution destination of EKB. The data pointer 63 is a pointer in which the position of the data division 66 in EKB is shownand the tag pointer 64 and the signature pointer 65 are pointers in which the position of the tag part 67 and the signature 68 is shownrespectively.

[0066]The data produced byfor examplethe node key to update being enciphered is stored in the data division 66. For exampleeach cryptographic key about the updated node key as shown in drawing 9 is stored in the data division 66.

[0067]The tag part 67 is a tag which was stored in the data division 66 and in which the physical relationship of the node key and leaf key which were enciphered is shown. The grant rule of this tag is explained with reference to drawing 11.

[0068]In the example of drawing 11as shown in drawing 11 Blet the data sent be a cryptographic key of drawing 7. Let the address of the top node contained in a cryptographic key be a top node address.

[0069]In this examplesince updating key K(t) R of the route key is containeda top node address serves as KR. At this timethe data Enc (K(t) 0 and K (t) R) of the highest rung corresponds to the position P0 shown in the class tree shown in drawing 11 Afor example. The data of the following stage is Enc (K (t) 00K(t)0)and corresponds to the position P00 at the lower left of the front data Enc (K(t) 0 and K (t) R) on a tree.

[0070]That iswhen it sees from the position of a tree structure and data is in the bottom of ita tag is set as 0and when there is no dataa tag is set as 1. A tag is set up as {a left (L) tag and a right (R) tag}.

[0071]Since it is set to L tag =0 since there is data in the position P00 at the lower left of the position P0 corresponding to the data Enc (K(t) 0 and K (t) R) of the highest rung of drawing 11 Band there is no data in the lower right of the position P0it is set to R tag =1. Hereaftera tag is set as all the data and the data row shown in drawing 11 C and a tag sequence are constituted.

[0072]A tag is set up in order that the corresponding data Enc (KxxxKyyy) may show where [of a tree structure] it is located. the key data Enc (KxxxKyyy) stored in the data division 66 -- although ... is only enumeration data of the key enciphered simplydistinction of the position on the tree of the cryptographic key stored as data of it is attained with the tag mentioned above. Without using a

tagas shown in drawing 7 or drawing 8the node index to which encryption data was made to correspond is usedfor example0:Enc(K(t) 0 and K (t) R)00:Enc(K -- (-- t --) -- 00 -- K -- (-- t --) -- 0)000:Enc (K ((-- t --) -- 000 -- K -- (-- t --) -- 00)although it is also possible to consider it as a data configuration like ...) When it has composition using such an indexin the distribution etc. which the data volume increases and pass a networkit is not desirable. On the other handdistinction of the position of a key is attained with smaller data volume by using the above tags as index data in which the position of a key is shown.

[0073]Returning to explanation of drawing 10the signature (Signature) 68 is an electronic signature which published EKBfor examplea lock management center (license server 4)contents ROBAIDA (content server 3)a settlement-of-accounts organization (fee collection server 5)etc. perform. The device which received EKB judges whether acquired EKB is EKB which the just publisher published by verifying the signature included in EKB.

[0074]Drawing 12 is a figure in which the contents currently recorded on CD81 show typically the processing incorporated by the client 1 in the above key management systems.

[0075]CPU21 of the client 1 controls the ripping module 91 which comprises executing a predetermined programand makes the contents memorized by CD81 connected to the client 1 incorporate.

[0076]CPU21 makes the storage parts store 28 memorize the data obtained by adding content ID (CID) and ID (unique ID (Uniq ID)) set up as a peculiar thing to the client 1 to the contents incorporated with the ripping module 91. This unique ID is a random number which consists of a predetermined digit numberfor exampleand the same unique ID as what was added to contents is saved by the client 1.

[0077]CPU21 generates the right of use of the contents incorporated with the ripping module 91 as service in the key management system mentioned above. For examplewhen the contents from which the ripping module 91 was incorporated by that cause are the modules whose check-out is enabled only 3 timesthe right of use the service condition showing the ability to check out only 3 times was described to be is generated. The content ID and unique ID which were added to contents are also described by the right of useand matching of contents and the right of use is made.

[0078]In the client reproduced when reproducing the contents incorporated as mentioned aboveIt is not only judged whether reproduction is permitted by the right of usebut it is judged whether unique ID added to contents and unique ID of the client which reproduces the contents are the same. And regeneration of contents is performed only when unique ID which reproduction of contents is permitted by the right of useand is added to contentsand unique ID of the client which generates contents are the same. That isin the client which acquired only contents and the right of use by a copy etc.temporarilyeven if it is a case where reproduction is permitted by the right of usethe contents can be reproduced.

[0079]Hereaftercontents are incorporated and a series of processings of the client

1 using it are explained with reference to a flow chart.
[0080]Processing of the client 1 which incorporates contents is explained with reference to the flow chart of introduction and drawing 13.
[0081]For examplewhen it is directed that the drive 30 of the client 1 is equipped with predetermined recording mediasuch as CD81 (optical disc 42) on which contents were recordedand contents are incorporatedCPU21 of the client 1 controls the ripping module 91 which comprises executing a predetermined programand incorporates contents in Step S1.
[0082]CPU21 generates the content ID which identifies contents in Step S2. In Step S3CPU21 to the client 1 (ripping module 91) peculiar unique IDFor examplewhen it judges whether the storage parts store 28 memorizes and judges with it not being memorizedit progresses to step S4 and unique ID which consists of a predetermined digit number is generated. Generated unique ID is saved at the storage parts store 28.
[0083]It is not what was generated in the client 1 as unique IDFor examplewhen a user of the client 1 registers predetermined information into the license server 4 so that he may make the ripping module 91 availableit may be made to use what is given to the client 1 from the license server 4. Thuswhen unique ID is givenor when already being generated in ripping performed in the pastin Step S3 of drawing 13it is judged with there being unique ID and processing of step S4 is skipped.
[0084]CPU21 is described in Step S5 to "Attribute (attribute)" as a field where predetermined attribution information of contents is described in content ID and unique ID. A format of contents is explained in full detail behind.
[0085]In Step S6CPU21 creates a digital signature based on information described as attribution information using its own secret key. This secret key is provided from the license server 4for examplewhen information about the client 1 is registered.
[0086]In Step S7CPU21 creates the data of the header recorded corresponding to contents. The data of a header is constituted by URL showing the access point for acquiring content IDright-of-use IDand the right of useand the watermark.
[0087]CPU21 creates the digital signature based on the data of the header created by processing of Step S7 in Step S8 using its own secret key. CPU21 makes contents encipher in step S9 by the contents key which controlled and generated the encryption decoding part 24. Informationincluding the generated contentsthe header which accompanies itetc.is saved in Step S10 at the storage parts store 28.
[0088]Drawing 14 is a figure showing the example of a format of contents.
[0089]The data (Enc (KrootKc)) produced by contents enciphering a headerEKBand the contents key Kc by the route key Kroot as shown in drawing 14The attribution information content ID and unique ID are described to be (Attribute)A certificate (Cert)the digital signature generated based on the header (Sig (Header))It comprises the data (Enc (KcContent))the metadata (Meta Data)and the mark (Mark) which are produced by enciphering contents by the

contents key Kc.
[0090]Content ID (CID)right-of-use ID (right-of-use ID) which identifies the right of use corresponding to contentsURL showing the acquisition place (client 1) of the right of useand a watermark (WM) are described by the header.
[0091]Artist ID as identification information for identifying record company ID as identification information for identifying the donor of content ID and contents and an artistunique IDetc. are contained in the attribute of contents. In this examplesince the contents which are the targets of the right of use are specifiedan attribute is used.
[0092]Metadata is various kinds of information relevant to contentsfor examplethe data of a jacketa photographwordsetc. is added to contents as metadata to a music content. The digital signature generated based on a user's ID (leaf ID)an ownership flagbeginning-of-using timecopy frequencyand these information is described by the mark. The ownership flag of a mark is added when only a predetermined periodfor examplebuys the right of use which makes contents usable as it was (when duration of service is changed into a using [it]-eternally thing). Histories (log)such as the number of times which copied the contentsare described by the copy frequency of a mark.
[0093]Although the case where contents were acquired from CD81 above (ripping) was explainedFor exampleabout the contents acquired from the predetermined server via the Internet 2similarlyunique ID of the client 1 is added with content IDand it is saved by the client 1.
[0094]Nextwith reference to the flow chart of drawing 15processing of the client 1 which generates the right of use corresponding to the incorporated contents is explained.
[0095]In Step S21the right of use beforehand set up as what is given to the contents incorporated with the ripping module 91 is read from the storage parts store 28 as the right of use corresponding to the contents incorporated by processing of drawing 13. Informationincluding right-of-use IDa versionthe date and time of creationthe term of validityetc.is described by the right of use memorized by the storage parts store 28.
[0096]In Step S22only in the client 1 to which the same ID as unique ID described as attribution information of contents is setCPU21 adds the information showing the contents being renewable while adding unique ID to the selected right of use. In Step S23CPU21 chooses a service condition and adds it. For examplewhen it is set up that the contents incorporated by that cause can check out only 3 times simultaneously to the ripping module 91the service condition showing the ability to check out only 3 times is chosen. When it is set up that the contents incorporated by that cause can copy freely to the ripping module 91 for examplethe service condition showing it is chosen.
[0097]In Step S24CPU21 creates the digital signature of the data described by the right of use selected as mentioned aboveand adds it. The right of use to which the digital signature was added is saved in Step S25 at the storage parts store 28.
[0098]Drawing 16 is a figure showing the example of a format of the right of use.

[0099]A version is information which divides a major version and a minor version by a dotand describes the version of the right of use. A profile is information which is described from the integral value of a decimal and specifies the restriction to the describing method of the right of use. Right-of-use ID is identification information for identifying the right of use described by a hexadecimal constant. The date and time of creation shows the date on which the right of use was created. The term of validity shows the term of validity of the right of use. It is shown that the term of validity which is 59 minutes and 59 seconds will not have restriction in the term of validity at 23:00 in 9999. The expiration date which can use contents for a service condition based on the right of useThe reproduction term which can reproduce contents based on the right of useThe number of times which can copy contents based on the maximum reproduction frequency of contentsand its right of use (copy frequency allowed)The information which shows the number of times which can be copied [whether contents are recordable on CD-R and] to PD (Portable Device) based on the number of times of the maximum check-out and its right of usethe propriety of movement of the right of usethe existence of duty to take a use logetc. is included. The electronic signature of a service condition is an electronic signature corresponding to a service condition.

[0100]A constant is a constant referred to by the service condition or a busy condition. Unique ID is generated when incorporating contents. An electronic signature is an electronic signature corresponding to the whole right of use. A certificate is a certificate containing the public key of the license server 4.

[0101]In accordance with the service condition of the right of usethe busy condition (contents conditions) which is the information showing the state of contents or the right of use is memorized by the storage parts store 28 of the client 1. The number of times which reproduced contents based on the right of use corresponding to a busy conditionThe information which shows the hysteresis information about the number of times which copied contentsthe number of times which checked out contentsthe first time to reproduce contentsthe number of times which recorded contents on CD-Rother contentsor the right of useetc. is included. The judgment of the conditions of reproduction of contents is performed based on the service condition included in the right of useand the busy condition memorized by the storage parts store 28 with the right of use. For examplewhen there is less number of times which reproduced the contents memorized by the busy condition than the contents maximum reproduction frequency contained in a service conditionit is judged with reproductive conditions being fulfilled.

[0102]Nextwith reference to the flow chart of drawing 17the regeneration of contents by the client 1 which incorporated contents with the ripping module 91 is explained.

[0103]In Step S41CPU21 of the client 1 reads unique ID described as attribution information of the contents which read and read the contents to which it pointed because a user operates the input part 26 from the storage parts store 28 based on content ID. CPU21 reads unique ID which reads the right of use corresponding

to the contents reproduction was instructed to be based on right-of-use IDand is described by the read right of use in Step S42.
[0104]Unique ID which CPU21 saved in Step S43Namelyunique ID of the client 1 is read from the storage parts store 28It progresses to Step S44 and it is judged whether all of unique ID described by those unique IDi.e.unique ID described by contentsand the right of use and unique ID saved at the client 1 are the same. It may be made to be judged whether only unique ID described by contents and unique ID saved at the client 1 are the same.
[0105]When it judges with all the unique ID of CPU21 being the same in Step S44it progresses to Step S45 and it is judged by the right of use whether use of contents is permitted based on the service condition described. For exampleCPU21 judges whether the term of validity (refer to drawing 16) as a descriptive content of the right of use and use of whether the right of use is a thing within the term of validity by comparing the present date clocked by the timer 20 and contents are permitted.
[0106]In Step S45when judged with use being permitted by the right of useit progresses to Step S46 and CPU21 performs processing which decodes contents (read) memorized by RAM23. Contents decoding processing performed in Step S46 is later mentioned with reference to a flow chart of drawing 18.
[0107]CPU21 supplies contents decoded by the encryption decoding part 24 to the codec part 25and makes them decode in Step S47. And CPU21 supplies and carries out digital to analog conversion of the data decoded by the codec part 25 to the outputting part 27 via the input/output interface 32and is made to output from a loudspeaker.
[0108]Unique ID described by contents at Step S44When judged with unique ID (unique ID further described by the right of use) saved at the client 1 differingat Step S45. When judged with reproduction of contents not being permitted by the right of usein Step S48error handling is performed and processing is ended after that.
[0109]Nextwith reference to the flow chart of drawing 18the details of the decoding processing of the client performed in Step S46 of drawing 17 are explained.
[0110]In Step S61by DNK which was contained in service information and provided from the license server 4CPU21 of the client 1 decodes the key information included in EKB one by oneand acquires the route key Kroot (KR). It progresses to Step S62 and CPU21 decodes the contents key Kc using the route key Krootwhen the route key Kroot is acquired. As shown in drawing 14the data Enc (KrootKc) produced by the contents key Kc being enciphered by the route key Kroot is added to contents.
[0111]In Step S63CPU21 decodes contents by the contents key Kc acquired at Step S62.
[0112]Drawing 19 expresses the above decoding processing typically. In drawing 19contents are saved by the client 1 and only the main information is shown among the information shown in drawing 14.

[0113]By namelythe route key Kroot which the route key Kroot was acquired (Step S61 of drawing 18)and was acquired from EKB based on DNK with which the client 1 was provided from the license server 4. The data Enc (KrootKc) is decoded andtherebythe contents key Kc is acquired (Step S62 of drawing 18). And the data Enc (KcContent) is decoded by the contents key Kcand the contents (Content) are acquired (Step S63 of drawing 18). As shown in drawing 20the data Enc (DNKKroot) produced by the route key Kroot being enciphered by DNK is contained in EKB of drawing 14 and drawing 19.
[0114]Contents can be reproduced even if it is the client (client by which unique ID is not managed) which acquired the right of use unjustly with contents by controlling reproduction of contents as mentioned above.
[0115]When it is carried out that the contents incorporated by the client 1 by the above processing can check out (when it is set up as a service condition that he can check out)To other clients which receive check-out of contents from the client 1it is enciphered by a predetermined method and contentsthe right of useand unique ID of the client 1 may be made to provide. In that casein the client which received offer of those informationthe same processing as what is shown in drawing 17 and drawing 18 is performedand reproduction of contents is performed. Therebycheck-out/check-in of the contents under management of the client 1 from which contents were incorporated first are performed.
[0116]In the above-mentioned embodimentsince the right of use required in order to use contents was specifiedthe contents conditions of the attribute of contents and the right of use were usedbut it does not restrict to this. For examplesince it is decided that the right of use required if it may be made for right-of-use ID of the right of use required in order to use these contents to be included in contents and contents are specified as them in this casein order to use it will be a meaningit does not need to perform processing which determines both matching.
[0117]
[Effect of the Invention]According to this inventioncontents can be provided.
[0118]According to this inventionuse of inaccurate contents can be prevented.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a mimetic diagram of the managerial system of the conventional contents.
[Drawing 2]It is a figure showing the example of composition of the contents providing system which applied this invention.
[Drawing 3]It is a block diagram showing the example of composition of the client of drawing 2.
[Drawing 4]It is a figure showing the composition of a key.
[Drawing 5]It is a figure showing a category node.
[Drawing 6]It is a figure showing the example of correspondence of a node and a

device.
[Drawing 7]It is a figure showing the example of composition of validation key blocks.
[Drawing 8]It is a figure showing other examples of composition of validation key blocks.
[Drawing 9]It is the figure which expressed use of validation key blocks typically.
[Drawing 10]It is a figure showing the example of a format of validation key blocks.
[Drawing 11]It is a figure explaining the composition of the tag of validation key blocks.
[Drawing 12]It is a mimetic diagram of the managerial system of the contents which applied this invention.
[Drawing 13]It is a flow chart explaining contents incorporation processing of the client of drawing 1.
[Drawing 14]It is a figure showing the example of a format of contents.
[Drawing 15]It is a flow chart explaining the right-of-use generation processing of the client of drawing 1.
[Drawing 16]It is a figure showing the example of a format of the right of use.
[Drawing 17]It is a flow chart explaining contents playback processing of the client of drawing 1.
[Drawing 18]It is a flow chart explaining the details of the decoding processing in Step S46 of drawing 17.
[Drawing 19]It is the figure which expressed the decoding processing of drawing 18 typically.
[Drawing 20]It is a figure showing the example of the information included in EKB of drawing 19.
[Explanations of letters or numerals]
1-11-2 [A timer21CPUand 24 / An encryption decoding part25 codec partsand 26 / An input part27 outputting partsand 28 / A storage parts store and 29 / Communications department] A clientthe 2 Internetand 3 A content server and 4 A license server5 fee-collection serverand 20

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－317376
（P2003－317376A）
(43)公開日　平成15年11月７日(2003.11.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｚ	５Ｃ０６４
Ｈ０４Ｎ　7/173	６４０	Ｈ０４Ｎ　7/173	６４０Ａ	５Ｄ０４４

審査請求　未請求　請求項の数７　ＯＬ　（全 17 頁）

(21)出願番号　特願2002－111555(P2002－111555)
(22)出願日　平成14年４月15日(2002.4.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　川本　洋志
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　情報管理装置および方法、記録媒体、並びにプログラム

(57)【要約】
【課題】　コンテンツの不正な利用を防止する。
【解決手段】　クライアント１のリッピングモジュール９１により、CD８１に記録されているコンテンツが取り込まれ、記憶部２８に保存される。クライアント１においては、コンテンツを識別するコンテンツID（CID）と、クライアント１（リッピングモジュール９１）に対して固有のユニークID（Uniq ID）が生成され、それらのIDが、リッピングモジュール９１により取り込まれたコンテンツに付加される。また、クライアント１においては、コンテンツの使用条件等が記述された利用権が生成され、保存される。利用権には、コンテンツに付加されているユニークIDと同一のIDが設定されている装置（クライアント）のみでのコンテンツの再生を許可することを表す情報が記述される。本発明は、パーソナルコンピュータなどの情報処理装置に適用することができる。

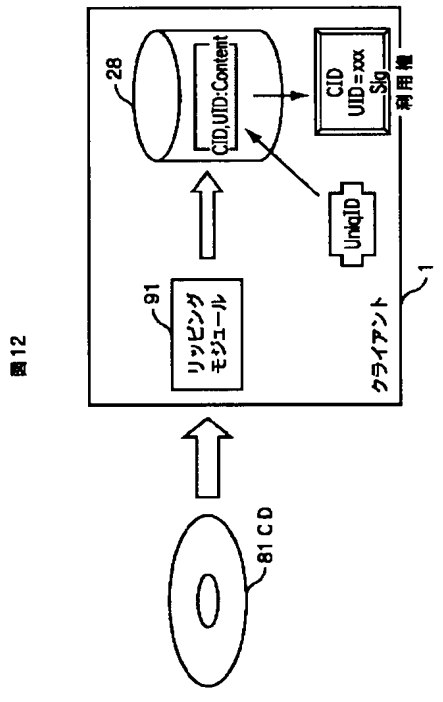


図12

【特許請求の範囲】

【請求項１】　コンテンツを管理する情報管理装置において、前記コンテンツを取得するコンテンツ取得手段と、前記情報管理装置を識別する識別情報を取得する識別情報取得手段と、前記コンテンツ取得手段により取得された前記コンテンツに、前記識別情報取得手段により取得された前記識別情報を付加して記憶するコンテンツ記憶手段と、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶手段とを備えることを特徴とする情報管理装置。

【請求項２】　前記コンテンツに付加されている前記識別情報と、前記識別情報取得手段により取得された前記識別情報が同一であるとき、前記コンテンツを再生する再生手段をさらに備えることを特徴とする請求項１に記載の情報管理装置。

【請求項３】　前記コンテンツ取得手段は、前記情報管理装置に装着された所定の記録媒体から前記コンテンツを取得することを特徴とする請求項１に記載の情報管理装置。

【請求項４】　前記識別情報取得手段は、生成した乱数を前記識別情報とすることを特徴とする請求項１に記載の情報管理装置。

【請求項５】　コンテンツを管理する情報管理装置の情報管理方法において、前記コンテンツを取得するコンテンツ取得ステップと、前記情報管理装置を識別する識別情報を取得する識別情報取得ステップと、前記コンテンツ取得ステップの処理により取得された前記コンテンツに、前記識別情報取得ステップの処理により取得された前記識別情報を付加して記憶するコンテンツ記憶ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶ステップとを含むことを特徴とする情報管理方法。

【請求項６】　コンテンツを管理する情報管理装置の記録媒体において、前記コンテンツの取得を制御するコンテンツ取得制御ステップと、前記情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、前記コンテンツ取得制御ステップの処理により取得された前記コンテンツに、前記識別情報取得制御ステップの処理により取得された前記識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項７】　コンテンツを管理する情報管理装置を制御するコンピュータに、前記コンテンツの取得を制御するコンテンツ取得制御ステップと、前記情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、前記コンテンツ取得制御ステップの処理により取得された前記コンテンツに、前記識別情報取得制御ステップの処理により取得された前記識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、前記コンテンツの利用に関する情報として、前記識別情報と、前記コンテンツに付加されている前記識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップとを実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報管理装置および方法、記録媒体、並びにプログラムに関し、特に、コンテンツの不正な再生を容易に防止できるようにする情報管理装置および方法、記録媒体、並びにプログラムに関する。

【０００２】

【従来の技術】近年、各種のブロードバンド環境が整備されつつあり、音楽データや動画データなどの各種のコンテンツの配信サービスが本格的に開始され始めている。

【０００３】例えば、「PressPlay（商標）」などの定期購読型（subscription型）の音楽配信サービスが行われており、この音楽配信サービスにおいては、ユーザは、月極の定額の料金を支払うことで、予め設定されている条件の範囲内（例えば、ストリーミング再生の場合１０００曲まで再生可能、ダウンロードしてパーソナルコンピュータのハードディスクに保存する場合１００曲まで保存可能、CD(Compact Disk)-Rへの書き込み（コピー）する場合２０曲までコピー可能などの条件の範囲内）で音楽コンテンツを利用することができる。

【０００４】ところで、このような配信サービスによるコンテンツの提供を受けるユーザの権利情報を管理するシステムとして、例えば、特開平２００１－３５２３２１号公報には、複数のサービスに対応するノードをツリー状に配置してなるシステムにおいて、所定のサービスに対応するノードから、そのサービスに属するそれぞれのリーフのノード（デバイス）までのパス上に存在するノードに設定されている鍵情報（DNK(Device Node Key)）を含む有効化キーブロック（EKB(Enabling Key Block)）を用いることが開示されている。

【０００５】このシステムでは、あるサービスにおいて配信されるコンテンツにEKBが付加されており、個々のデバイスに対して与えられているDNKを利用して、EKBに含まれる、更新された鍵情報を取得させることにより、

サービスの利用を許可するデバイスを管理している。この場合において、DNKを利用して、EKBから、更新された鍵情報を取得できないデバイスは、その後、サービスの提供を受けることができない。

【０００６】そして、これにより、コンテンツを提供するサーバとデバイスとの間で認証処理などをその都度行うことなく、それぞれのデバイスにおけるコンテンツの利用を管理できるようにしたものである。

【０００７】また、このようにしてコンテンツの権利情報が管理されるシステムにおいては、例えば、CD(Compact Disk)からコンテンツをインポートしたデバイスは、そのコンテンツをICV(Integrity Check Value)により管理するようになされている。

【０００８】図１は、インポートしたコンテンツをICVにより管理する構成を模式的に示す図である。

【０００９】図１に示されるように、例えば、パーソナルコンピュータなどのデバイスは、CDからインポートしたコンテンツ（音楽データ）をハードディスクの管理テーブルに登録し、登録されているコンテンツに基づいて生成されたMAC(Message Authentication Code)（Ｃ１，Ｃ２，…，Ｃｎ）をICV＝hash(Ｋｉｃｖ，Ｃ１，Ｃ２，…，Ｃｎ)に適用し、ICVを生成する。なお、ＫｉｃｖはICVを生成するための鍵情報である。

【００１０】そして、コンテンツ生成時に生成し、安全に保存しておいたICVと、再生時などの所定のタイミングで新たに生成したICVとを比較し、同一のICVが得られれば、コンテンツに改竄がなかったと判定され、一方、得られたICVがコンテンツ生成時のものと異なる場合、コンテンツに改竄があったと判定される。コンテンツに改竄がなかったと判定された場合、続けて、コンテンツの再生処理が行われ、改竄があったと判定された場合、再生処理は行われない。従って、これにより、改竄されたコンテンツの再生が防止される。

【００１１】

【発明が解決しようとする課題】しかしながら、以上のようにしてICVによりコンテンツを管理する場合、コンテンツをインポートする毎に、或いはコンテンツを再生する毎にICVを生成しなければならず、その処理負担が大きいという課題があった。

【００１２】従って、音楽再生用デバイスなどのポータブルデバイスにとっては、ICVを生成するためのハッシュ演算が可能な高性能の演算部が必要となり、そのような演算部を設けるようにした場合、結果として、デバイスのコストが上がることとなる。

【００１３】本発明はこのような状況に鑑みてなされたものであり、コンテンツの不正な再生を容易に防止できるようにするものである。

【００１４】

【課題を解決するための手段】本発明の情報管理装置は、コンテンツを取得するコンテンツ取得手段と、情報管理装置を識別する識別情報を取得する識別情報取得手段と、コンテンツ取得手段により取得されたコンテンツに、識別情報取得手段により取得された識別情報を付加して記憶するコンテンツ記憶手段と、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶手段とを備えることを特徴とする。

【００１５】コンテンツを再生する再生手段がさらに設けられ、その再生手段が、コンテンツに付加されている識別情報と、識別情報取得手段により取得された識別情報が同一であるときにのみコンテンツを再生するようにしてもよい。

【００１６】コンテンツ取得手段は、情報管理装置に装着された所定の記録媒体からコンテンツを取得することを特徴とする。

【００１７】識別情報取得手段は、自分自身が生成した乱数を識別情報として、コンテンツ等に付加するようにしてもよい。また、識別情報は外部の装置などから提供されるものであってもよい。

【００１８】本発明の情報管理装置の情報管理方法は、コンテンツを取得するコンテンツ取得ステップと、情報管理装置を識別する識別情報を取得する識別情報取得ステップと、コンテンツ取得ステップの処理により取得されたコンテンツに、識別情報取得ステップの処理により取得された識別情報を付加して記憶するコンテンツ記憶ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権を記憶する利用権記憶ステップとを含むことを特徴とする。

【００１９】本発明の情報管理装置の記録媒体には、コンテンツの取得を制御するコンテンツ取得制御ステップと、情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、コンテンツ取得制御ステップの処理により取得されたコンテンツに、識別情報取得制御ステップの処理により取得された識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権の記憶を制御する利用権記憶制御ステップを、コンピュータに実行させるプログラムが記録されていることを特徴とする。

【００２０】本発明のプログラムは、コンテンツを管理する情報管理装置を制御するコンピュータに、コンテンツの取得を制御するコンテンツ取得制御ステップと、情報管理装置を識別する識別情報の取得を制御する識別情報取得制御ステップと、コンテンツ取得制御ステップの処理により取得されたコンテンツに、識別情報取得制御

ステップの処理により取得された識別情報を付加して行う記憶を制御するコンテンツ記憶制御ステップと、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が設定されている装置での利用を許可する情報が含まれている利用権情報の記憶を制御する利用権記憶制御ステップとを実行させることを特徴とする。

【００２１】本発明の情報管理装置および方法、並びにプログラムにおいては、コンテンツが取得され、情報管理装置を識別する識別情報が取得される。また、取得されたコンテンツに対して、取得された識別情報が付加されて記憶され、コンテンツの利用に関する情報として、識別情報と、コンテンツに付加されている識別情報と同一の識別情報が取得されている装置での利用を許可する情報が含まれている利用権が記憶される。

【００２２】

【発明の実施の形態】図２は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット２には、クライアント１－１，１－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１と称する）が接続されている。この例においては、クライアントが２台のみ示されているが、インターネット２には、任意の台数のクライアントが接続される。

【００２３】また、インターネット２には、クライアント１に対してコンテンツを提供するコンテンツサーバ３、コンテンツサーバ３が提供するコンテンツを利用するのに必要な利用権をクライアント１に対して付与するライセンスサーバ４、およびクライアント１が利用権を受け取った場合に、そのクライアント１に対して課金処理を行う課金サーバ５が接続されている。

【００２４】これらのコンテンツサーバ３、ライセンスサーバ４、および課金サーバ５も、任意の台数だけ、インターネット２に接続される。

【００２５】図３はクライアント１の構成を表している。

【００２６】図３において、CPU（Central Processing Unit）２１は、ROM（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からRAM（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をCPU２１に供給する。RAM２３にはまた、CPU２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００２７】暗号化復号部２４は、コンテンツを暗号化するとともに、既に暗号化されているコンテンツを復号する処理を行う。コーデック部２５は、例えば、ATRAC（Adaptive Transform Acoustic Coding）３方式などでコンテンツをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。半導体メモリ４４は、例えば、メモリスティック（商標）などにより構成される。

【００２８】CPU２１、ROM２２、RAM２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

【００２９】入出力インタフェース３２には、キーボード、マウスなどよりなる入力部２６、CRT(Cathode Ray Tube)、LCD(Liquid Crystal Display)などよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、モデム、ターミナルアダプタなどより構成される通信部２９が接続されている。通信部２９は、インターネット２を介しての通信処理を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【００３０】入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

【００３１】なお、図示は省略するが、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５も、図３に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図３の構成は、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５などの構成としても引用される。

【００３２】本発明においては、図４に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイス固有のキーに対応する。本発明のシステムに用いられる階層ツリー構造鍵管理については特開２００１－３５２３２１号公報に記載されている。図４の例の場合、番号０から番号１５までの１６個のデバイスに対応するキーが生成される。

【００３３】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKR（適宜、Ｋｒｏｏｔとも称する）が規定され、２段目のノードに対応してキーＫ０，Ｋ１が規定される。また、３段目のノードに対応してキーＫ００乃至Ｋ１１が規定され、第４段目のノードに対応してキーＫ０００乃至キーＫ１１１が規定される。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーＫ０００００乃至Ｋ１１１１が、

それぞれ対応されている。

【００３４】階層構造とされているため、例えば、キーＫ００１０とキーＫ００１１の上位のキーは、Ｋ００１とされ、キーＫ０００とキーＫ００１の上位のキーは、Ｋ００とされている。以下、同様に、キーＫ００とキーＫ０１の上位のキーは、Ｋ０とされ、キーＫ０とキーＫ１の上位のキーは、KRとされている。

【００３５】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの１つのパスの各ノードに対応するキーで管理される。例えば、番号３のリーフに対応するデバイスにおいて、コンテンツを利用するためのキーは、キーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，KRを含むパスの各キーで管理される。

【００３６】本発明のシステムにおいては、図５に示されるように、図４の原理に基づいて構成されるキーシステムで、デバイスのキーとコンテンツのキーの管理が行われる。図５の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、或いは、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの１つのノードに、利用権を管理するシステムとして本システム（適宜、Ｔシステムと称する）が対応する。

【００３７】すなわち、Ｔシステムのノードよりさらに下の階層の２４段のノードに対応するキーにより、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスが対応される。従って、図５の例においては、2^{24}（約１６メガ）のサービスプロバイダ、あるいはサービスを規定することができる。また、最下段の３２段の階層により、2^{32}（約４ギガ）のユーザ（クライアント１）を規定することができる。最下段の３２段のノードからＴシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【００３８】コンテンツを暗号化したコンテンツキーは更新されたルートキーKR′によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB（Enabling Key Block：有効化キーブロック）（図７を参照して後述する）内に配置される。

【００３９】EKBにおける末端から１つ上の段の更新ノードキーはEKBの末端のノードキーあるいはリーフキーによって暗号化され、EKB内に配置される。クライアント１は、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツとともに配布されるEKBに記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たノードキーを用いて、EKBに記述されている、さらにその上の階層の更新ノードキーを復号する。同様の処理を順次行うことで、クライアント１は、更新ルートキーKR′を得ることができる。サービスデータは、クライアント１についての情報を登録したときにライセンスサーバ４から供給されるものであり、このサービスデータと、後述する、特定のコンテンツの利用を許可する情報である利用権の組み合わせをライセンスと呼ぶ。

【００４０】図６は、階層ツリー構造のカテゴリの分類の具体的な例を示す図である。

【００４１】図６において、階層ツリー構造の最上段には、ルートキーKR２３０１が設定され、以下の中間段にはノードキー２３０２が設定され、最下段には、リーフキー２３０３が設定される。各デバイスは、個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーからなるデバイスノードキー（DNK）を保有する。

【００４２】最上段から第Ｍ段目（図５の例では、Ｍ＝８）の所定のノードがカテゴリノード２３０４として設定される。すなわち、第Ｍ段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第Ｍ段の１つのノードを頂点としてＭ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【００４３】例えば、図６の第Ｍ段目の１つのノード２３０５にはカテゴリ［メモリスティック（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード２３０５以下が、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【００４４】Ｍ段から数段分下位の段をサブカテゴリノード２３０６として設定することができる。図６の例では、カテゴリ［メモリスティック］ノード２３０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノード２３０６が設定されている。また、サブカテゴリノードである再生専用器のノード２３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード２３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［PHS］ノード２３０８と、［携帯電話］ノード２３０９が設定されている。

【００４５】カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えば、あるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、或いは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。

【００４６】例えば、１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定することにより、メーカーの販売するゲーム機器XYZに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することができ、その後、その頂点ノードキー以下のノードキー、リーフキーによって構成されるEKBを生成して配信することで、暗号化コンテンツの配信処理、各種キーの配信処理、更新処理等を、頂点ノード以下のデバイス（ゲーム機器XYZ）に対してのみ行うことができる。

【００４７】すなわち、頂点ノードに属さない、他のカテゴリのノードに属するデバイスには全く影響を及ぼすことなく、キーの更新等を実行することができる。

【００４８】また、ある時点ｔにおいて、デバイス３の所有する鍵Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキーＫ００１，Ｋ００，Ｋ０，KRを、それぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）ｔの更新キーであることを示す。

【００４９】更新キーの配布処理ついて説明する。キーの更新は、例えば、図７に示されるEKBによって構成されるテーブルを、ネットワークを介して、あるいは所定の記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、EKBは、図４に示されるようなツリー構造を構成する各リーフ（最下段のノード）に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。

【００５０】図７に示されるEKBは、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図７の例は、図４に示されるツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。

【００５１】図４から明らかなように、デバイス０，１に対しては、更新ノードキーとしてＫ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを提供することが必要であり、デバイス２に対しては、更新ノードキーとしてＫ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを提供することが必要である。

【００５２】図７のEKBに示されるように、EKBには複数の暗号化キーが含まれ、例えば、図７の最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これは、デバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自分自身が有するリーフキーＫ００１０によって、暗号化キーを復号し、更新ノードキーＫ（ｔ）００１を取得できる。

【００５３】また、デバイス２は、復号により得た更新ノードキーＫ（ｔ）００１を用いて、図７の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号することができ、更新ノードキーＫ（ｔ）００を取得することができる。

【００５４】デバイス２は、同様に、図７の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０を取得でき、これを用いて、図７の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒを取得できる。

【００５５】一方、ノードキーＫ０００は、更新する対象のキーに含まれておらず、ノード０，１が更新ノードキーとして必要なのは、Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒである。

【００５６】ノード０，１は、デバイスキーＫ０００００，Ｋ０００１を用いて、図７の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号することにより更新ノードキーＫ（ｔ）００を取得し、同様に、順次、図７の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号することで、更新ノードキーＫ（ｔ）０を取得し、さらに、図７の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号することで、更新ルートキーＫ（ｔ）Ｒを取得する。このようにして、デバイス０，１，２は、更新したキーＫ（ｔ）Ｒを得ることができる。

【００５７】なお、図７のインデックスは、図の右側に示される暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００５８】図４に示されるツリー構造の上位段のノードキーＫ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図８のEKBを用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００５９】図８に示されるEKBは、例えば、特定のグループにおいて共有される新たなコンテンツキーを配布する場合に利用可能である。

【００６０】例えば、図４の一点鎖線で示されるグループ内のデバイス０，１，２，３が、ある記録媒体を用いており、それらのデバイスに対して新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを設定することが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００により、新たな共通の更新コンテンツキーＫ（ｔ）ｃｏｎが暗号化されたデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）が、図８に示されるEKBとともに配布される。この配布により、デバイス４など、その他のグループの機器が復号す

ることができないデータとしての配布が可能となる。

【００６１】すなわち、デバイス０，１，２は、EKBを処理して得たキーＫ（ｔ）００を用いて暗号データを復号することで、ｔ時点におけるコンテンツキーＫ（ｔ）ｃｏｎを得ることができる。

【００６２】図９は、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理の例として、Ｋ（ｔ）００により新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが暗号化されたデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と、図８に示されるEKBが、所定の記録媒体を介して提供されたデバイス０の処理を模式的に示す図である。すなわち、図９の例は、EKBによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００６３】図９に示されるように、デバイス０は、記録媒体に格納されている世代t時点のEKBと、自分自身に予め用意されているノードキーＫ０００を用いて、上述したようなEKB処理（鍵を順次解く処理）により、ノードキーＫ（ｔ）００を生成する。また、デバイス０は、復号した更新ノードキーＫ（ｔ）００を用いて、更新コンテンツキーＫ（ｔ）ｃｏｎを復号し、それを後に使用するために、自分だけが有するリーフキーＫ０００００で、更新コンテンツキーＫ（ｔ）ｃｏｎを暗号化して格納する。

【００６４】図１０は、EKBのフォーマットの例を示す図であり、このような各種の情報からなるEKBが、コンテンツデータのヘッダに含まれる。

【００６５】バージョン６１は、EKBのバージョンを示す識別子である。このバージョン６１は、最新のEKBを識別する機能と、コンテンツとの対応関係を示す機能を有する。デプス６２は、EKBの配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６３は、EKB中のデータ部６６の位置を示すポインタであり、タグポインタ６４および署名ポインタ６５は、タグ部６７および署名６８の位置をそれぞれ示すポインタである。

【００６６】データ部６６には、例えば、更新するノードキーが暗号化されて得られたデータが格納される。例えば、図９に示されるような、更新されたノードキーに関する各暗号化キー等がデータ部６６に格納される。

【００６７】タグ部６７は、データ部６６に格納された、暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを、図１１を参照して説明する。

【００６８】図１１の例においては、送付されるデータは、図１１Ｂに示されるように、図７の暗号化キーとされている。なお、暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。

【００６９】この例においては、ルートキーの更新キーＫ（ｔ）Ｒが含まれているため、トップノードアドレスはKRとなる。このとき、例えば、最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図１１Ａに示す階層ツリーに示す位置Ｐ０に対応する。次の段のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左下の位置Ｐ００に対応する。

【００７０】すなわち、ツリー構造の所定の位置から見て、その下にデータがある場合には、タグが０に設定され、データがない場合には、タグが１に設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。

【００７１】図１１Ｂの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）に対応する位置Ｐ０の左下の位置Ｐ００にはデータがあるため、Ｌタグ＝０となり、位置Ｐ０の右下にはデータがないため、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図１１Ｃに示すデータ列、およびタグ列が構成される。

【００７２】タグは、対応するデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）が、ツリー構造のどこに位置しているのかを示すために設定される。データ部６６に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）・・・は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによって、データとして格納された暗号化キーのツリー上の位置が判別可能となる。タグを用いずに、図７または図８に示されるように、暗号化データに対応させたノード・インデックスを用いて、例えば、０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（ｔ）００）・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とした場合、そのデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、以上のようなタグを、キーの位置を示す索引データとして用いることにより、より少ないデータ量で、キーの位置の判別が可能となる。

【００７３】図１０の説明に戻り、署名（Signature）６８は、EKBを発行した、例えば、鍵管理センタ（ライセンスサーバ４）、コンテンツロバイダ（コンテンツサーバ３）、決済機関（課金サーバ５）等が実行する電子署名である。EKBを受領したデバイスは、EKBに含まれる署名を検証することにより、取得したEKBが、正当な発行者が発行したEKBであるか否かを判定する。

【００７４】図１２は、以上のような鍵管理システムにおいて、CD８１に記録されているコンテンツが、クライアント１により取り込まれる処理を模式的に示す図である。

【００７５】クライアント１のCPU２１は、所定のプログラムを実行することで構成されるリッピングモジュール９１を制御し、クライアント１に接続されたCD８１に記憶されているコンテンツを取り込ませる。

【００７６】CPU２１は、リッピングモジュール９１により取り込まれたコンテンツに対して、コンテンツID

（CID）、およびクライアント１に対して固有のものとして設定されるID（ユニークID（Uniq ID））を付加し、得られたデータを記憶部２８に記憶させる。このユニークIDは、例えば、所定の桁数からなる乱数であり、コンテンツに付加されたものと同一のユニークIDがクライアント１により保存される。

【００７７】また、CPU２１は、上述した鍵管理システムにおけるサービスとしてのリッピングモジュール９１により取り込まれたコンテンツの利用権を生成する。例えば、リッピングモジュール９１が、それにより取り込まれたコンテンツが３回だけチェックアウトが可能とされるモジュールである場合、３回だけチェックアウトが可能であることを表す使用条件が記述された利用権が生成される。利用権には、コンテンツに対して付加されたコンテンツIDおよびユニークIDも記述され、コンテンツと利用権の対応付けがなされる。

【００７８】以上のようにして取り込まれたコンテンツを再生するとき、再生するクライアントにおいては、利用権により再生が許可されているか否かが判定されるだけでなく、コンテンツに付加されているユニークIDと、そのコンテンツを再生するクライアントのユニークIDが同一であるか否かが判定される。そして、利用権によりコンテンツの再生が許可され、かつ、コンテンツに付加されているユニークIDと、コンテンツを生成するクライアントのユニークIDが同一である場合にのみ、コンテンツの再生処理が行われる。すなわち、コンテンツと利用権のみをコピーなどにより取得したクライアントにおいては、仮に、利用権により再生が許可されている場合であっても、そのコンテンツを再生できないこととなる。

【００７９】以下、コンテンツを取り込み、それを利用するクライアント１の一連の処理について、フローチャートを参照して説明する。

【００８０】始めに、図１３のフローチャートを参照して、コンテンツを取り込むクライアント１の処理について説明する。

【００８１】例えば、コンテンツが記録されたCD８１（光ディスク４２）などの所定の記録媒体がクライアント１のドライブ３０に装着され、コンテンツを取り込むことが指示されたとき、クライアント１のCPU２１は、所定のプログラムを実行することで構成されるリッピングモジュール９１を制御し、ステップＳ１において、コンテンツを取り込む。

【００８２】CPU２１は、ステップＳ２において、コンテンツを識別するコンテンツIDを生成する。また、CPU２１は、ステップＳ３において、クライアント１（リッピングモジュール９１）に対して固有のユニークIDが、例えば、記憶部２８に記憶されているか否かを判定し、それが記憶されていないと判定した場合、ステップＳ４に進み、所定の桁数からなるユニークIDを生成する。生成されたユニークIDは、記憶部２８に保存される。

【００８３】なお、ユニークIDとして、クライアント１において生成されたものではなく、例えば、クライアント１のユーザが、リッピングモジュール９１を利用可能なものにするべく、所定の情報をライセンスサーバ４に登録したときに、ライセンスサーバ４からクライアント１に付与されるものを使用するようにしてもよい。このようにしてユニークIDが付与された場合、または、過去に行われたリッピングにおいて既に生成されている場合、図１３のステップＳ３において、ユニークIDがあると判定され、ステップＳ４の処理がスキップされる。

【００８４】CPU２１は、ステップＳ５において、コンテンツIDおよびユニークIDを、コンテンツの所定の属性情報が記述される領域としての「Attribute（属性）」に記述する。コンテンツのフォーマットについては後に詳述する。

【００８５】ステップＳ６において、CPU２１は、属性情報として記述されている情報に基づいたデジタル署名を、自分自身の秘密鍵を用いて作成する。この秘密鍵は、例えば、クライアント１に関する情報を登録したときにライセンスサーバ４から提供されたものである。

【００８６】ステップＳ７において、CPU２１は、コンテンツに対応して記録するヘッダのデータを作成する。ヘッダのデータは、コンテンツID、利用権ID、利用権を取得するためのアクセス先を表すURL、およびウォーターマークにより構成される。

【００８７】CPU２１は、ステップＳ８において、自分自身の秘密鍵を用いて、ステップＳ７の処理で作成したヘッダのデータに基づいたデジタル署名を作成する。CPU２１は、ステップＳ９において、暗号化復号部２４を制御し、生成したコンテンツキーでコンテンツを暗号化させる。生成されたコンテンツ、およびそれに付随するヘッダなどの情報は、ステップＳ１０において、記憶部２８に保存される。

【００８８】図１４は、コンテンツのフォーマットの例を示す図である。

【００８９】図１４に示されるように、コンテンツは、ヘッダ、EKB、コンテンツキーＫｃをルートキーＫｒｏｏｔで暗号化して得られるデータ（Enc（Ｋｒｏｏｔ，Ｋｃ））、コンテンツIDおよびユニークIDが記述される属性情報（Attribute）、証明書（Cert）、ヘッダに基づいて生成されたデジタル署名（Sig（Header））、コンテンツをコンテンツキーＫｃで暗号化して得られるデータ（Enc（Ｋｃ，Content））、メタデータ（Meta Data）、およびマーク（Mark）から構成される。

【００９０】ヘッダには、コンテンツID（CID）、コンテンツに対応する利用権を識別する利用権ID（利用権ID）、利用権の取得先（クライアント１）を表すURL、およびウォーターマーク（WM）が記述されている。

【００９１】コンテンツの属性には、コンテンツID、コンテンツの提供者を識別するための識別情報としてのレ

コードカンパニーID、アーティストを識別するための識別情報としてのアーティストID、および、ユニークIDなどが含まれる。本実施例では、属性は利用権の対象となるコンテンツを特定するために用いられる。

【００９２】なお、メタデータは、コンテンツに関連する各種の情報であり、例えば、音楽コンテンツに対しては、ジャケット、写真、歌詞等のデータがメタデータとしてコンテンツに付加される。また、マークには、ユーザのID（リーフID）、所有権フラグ、使用開始時刻、コピー回数、これらの情報に基づいて生成されたデジタル署名が記述される。マークの所有権フラグは、例えば、所定の期間だけコンテンツを使用可能とする利用権を、そのまま買い取ったような場合（使用期間を永久に使用できるのものに変更したような場合）に付加される。また、マークのコピー回数には、そのコンテンツをコピーした回数などの履歴（ログ）が記述される。

【００９３】以上においては、コンテンツがCD８１から取得（リッピング）される場合について説明したが、例えば、インターネット２を介して所定のサーバから取得されたコンテンツなどについても、同様に、コンテンツIDとともにクライアント１のユニークIDが付加されて、クライアント１により保存される。

【００９４】次に、図１５のフローチャートを参照して、取り込まれたコンテンツに対応する利用権を生成するクライアント１の処理について説明する。

【００９５】ステップＳ２１において、リッピングモジュール９１により取り込まれたコンテンツに対して付与するものとして予め設定されている利用権を、図１３の処理により取り込まれたコンテンツに対応する利用権として記憶部２８から読み出す。記憶部２８に記憶されている利用権には、利用権ID、バージョン、作成日時、有効期限等の情報が記述されている。

【００９６】ステップＳ２２において、CPU２１は、選択した利用権にユニークIDを付加するとともに、コンテンツの属性情報として記述されているユニークIDと同一のIDが設定されているクライアント１においてのみ、そのコンテンツを再生できることを表す情報を付加する。また、CPU２１は、ステップＳ２３において、使用条件を選択し、それを付加する。例えば、リッピングモジュール９１に対して、それにより取り込まれたコンテンツが同時に３回だけチェックアウトできることが設定されている場合、３回だけチェックアウトできることを表す使用条件が選択される。また、例えば、リッピングモジュール９１に対して、それにより取り込まれたコンテンツが自由にコピーできることが設定されている場合、それを表す使用条件が選択される。

【００９７】CPU２１は、ステップＳ２４において、以上のようにして選択した利用権に記述されているデータのデジタル署名を作成し、それを付加する。デジタル署名が付加された利用権は、ステップＳ２５において、記憶部２８に保存される。

【００９８】図１６は、利用権のフォーマットの例を示す図である。

【００９９】バージョンは、メジャーバージョンおよびマイナーバージョンをドットで区切って、利用権のバージョンを記述する情報である。プロファイルは、１０進の整数値から記述され、利用権の記述方法に対する制限を規定する情報である。利用権IDは、１６進定数で記述される、利用権を識別するための識別情報である。作成日時は、利用権が作成された日時を示す。有効期限は、利用権の有効期限を示す。９９９９年２３時５９分５９秒である有効期限は、有効期限に制限がないことを示す。使用条件には、その利用権に基づいて、コンテンツを使用することが可能な使用期限、その利用権に基づいて、コンテンツを再生することが可能な再生期限、コンテンツの最大再生回数、その利用権に基づいて、コンテンツをコピーすることが可能な回数（許されるコピー回数）、最大チェックアウト回数、その利用権に基づいて、コンテンツをCD-Rに記録することができるか否か、PD（Portable Device）にコピーすることが可能な回数、利用権の移動の可否、使用ログをとる義務の有無等を示す情報が含まれる。使用条件の電子署名は、使用条件に対応する電子署名である。

【０１００】定数は、使用条件または使用状態で参照される定数である。ユニークIDは、コンテンツを取り込むときに生成されたものである。電子署名は、利用権全体に対応する、電子署名である。証明書は、ライセンスサーバ４の公開鍵を含む証明書である。

【０１０１】また、クライアント１の記憶部２８には、利用権の使用条件とあわせて、コンテンツや利用権の状態を表す情報である使用状態（コンテンツ条件）が記憶される。使用状態には、対応する利用権に基づいてコンテンツを再生した回数、コンテンツをコピーした回数、コンテンツをチェックアウトした回数、コンテンツを初めて再生した日時、コンテンツをCD-Rに記録した回数、その他コンテンツあるいは利用権に関する履歴情報等を示す情報が含まれる。コンテンツの再生の条件の判定は、利用権に含まれる使用条件と、記憶部２８に利用権と共に記憶されている使用状態とを基に行われる。例えば、使用状態に記憶されているコンテンツを再生した回数が、使用条件に含まれるコンテンツ最大再生回数より少ない場合には、再生の条件が満たされていると判定される。

【０１０２】次に、図１７のフローチャートを参照して、リッピングモジュール９１によりコンテンツを取り込んだクライアント１による、コンテンツの再生処理について説明する。

【０１０３】ステップＳ４１において、クライアント１のCPU２１は、ユーザが入力部２６を操作することで指示したコンテンツをコンテンツIDに基づいて記憶部２８

から読み出し、読み出したコンテンツの属性情報として記述されているユニークIDを読み取る。また、CPU２１は、ステップＳ４２において、再生が指示されたコンテンツに対応する利用権を利用権IDに基づいて読み出し、読み出した利用権に記述されているユニークIDを読み取る。

【０１０４】ステップＳ４３において、CPU２１は、保存しておいたユニークID、すなわちクライアント１のユニークIDを記憶部２８から読み出し、ステップＳ４４に進み、それらのユニークID、すなわち、コンテンツに記述されているユニークID、利用権に記述されているユニークID、およびクライアント１に保存されているユニークIDが全て同じであるか否かを判定する。なお、コンテンツに記述されているユニークIDと、クライアント１に保存されているユニークIDのみが同一であるか否かが判定されるようにしてもよい。

【０１０５】CPU２１は、ステップＳ４４において、全てのユニークIDが同一であると判定した場合、ステップＳ４５に進み、利用権により、コンテンツの使用が許可されているか否かを、記述されている使用条件に基づいて判定する。例えば、CPU２１は、利用権の記述内容としての有効期限（図１６参照）と、タイマ２０により計時されている現在日時を比較することにより、利用権が有効期限内のものであるか否か、すなわち、コンテンツの使用が許可されているか否かを判定する。

【０１０６】ステップＳ４５において、利用権により使用が許可されていると判定された場合、ステップＳ４６に進み、CPU２１は、RAM２３に記憶された（読み出された）コンテンツを復号する処理を実行する。ステップＳ４６において行われるコンテンツ復号処理については、図１８のフローチャートを参照して後述する。

【０１０７】CPU２１は、ステップＳ４７において、暗号化復号部２４により復号されたコンテンツをコーデック部２５に供給し、デコードさせる。そして、CPU２１は、コーデック部２５によりデコードされたデータを、入出力インタフェース３２を介して出力部２７に供給し、ディジタルアナログ変換させ、スピーカから出力させる。

【０１０８】なお、ステップＳ４４で、コンテンツに記述されているユニークIDと、クライアント１に保存されているユニークID（さらに、利用権に記述されているユニークID）が異なると判定された場合、並びに、ステップＳ４５で、利用権によりコンテンツの再生が許可されていないと判定された場合、ステップＳ４８において、エラー処理が行われ、その後、処理が終了される。

【０１０９】次に、図１８のフローチャートを参照して、図１７のステップＳ４６において実行されるクライアントの復号処理の詳細について説明する。

【０１１０】ステップＳ６１において、クライアント１のCPU２１は、サービスデータに含まれてライセンスサーバ４から提供されたDNKにより、EKBに含まれる鍵情報を順次復号し、ルートキーＫｒｏｏｔ（KR）を取得する。CPU２１は、ルートキーＫｒｏｏｔを取得したとき、ステップＳ６２に進み、ルートキーＫｒｏｏｔを用いてコンテンツキーＫｃを復号する。図１４に示されるように、コンテンツには、コンテンツキーＫｃがルートキーＫｒｏｏｔにより暗号化されて得られたデータＥｎｃ（Ｋｒｏｏｔ，Ｋｃ）が付加されている。

【０１１１】ステップＳ６３において、CPU２１は、ステップＳ６２で取得したコンテンツキーＫｃによりコンテンツを復号する。

【０１１２】図１９は、以上の復号処理を模式的に表したものである。なお、図１９においては、コンテンツはクライアント１により保存されていたものであり、図１４に示される情報のうち、主な情報のみが示されている。

【０１１３】すなわち、ライセンスサーバ４からクライアント１に提供されたDNKに基づいて、EKBからルートキーＫｒｏｏｔが取得され（図１８のステップＳ６１）、取得されたルートキーＫｒｏｏｔにより、データＥｎｃ（Ｋｒｏｏｔ，Ｋｃ）が復号され、それによりコンテンツキーＫｃが取得される（図１８のステップＳ６２）。そして、コンテンツキーＫｃにより、データＥｎｃ（Ｋｃ，Content）が復号され、コンテンツ（Content）が取得される（図１８のステップＳ６３）。なお、図１４および図１９のEKBには、図２０に示されるように、ルートキーＫｒｏｏｔがDNKにより暗号化されて得られたデータＥｎｃ（DNK，Ｋｒｏｏｔ）が含まれている。

【０１１４】以上のようにしてコンテンツの再生を制御することにより、コンテンツとともに、利用権を不正に取得したクライアント（ユニークIDが管理されていないクライアント）であっても、コンテンツを再生できないこととなる。

【０１１５】また、以上の処理によりクライアント１により取り込まれたコンテンツがチェックアウトが可能であるとされている場合（チェックアウト可能であることが使用条件として設定されている場合）、クライアント１からコンテンツのチェックアウトを受ける他のクライアントに対しては、コンテンツ、利用権、およびクライアント１のユニークIDが所定の方法により暗号化されて提供されるようにしてもよい。その場合、それらの情報の提供を受けたクライアントにおいては、図１７および図１８に示されるものと同様の処理が実行され、コンテンツの再生が行われる。これにより、コンテンツが最初に取り込まれたクライアント１の管理下でのコンテンツのチェックアウト／チェックイン等が行われる。

【０１１６】また、上記実施例では、コンテンツを利用するために必要な利用権を特定するためにコンテンツの属性と利用権のコンテンツ条件を用いたが、これに限らない。例えば、コンテンツに、該コンテンツを利用する

ために必要な利用権の利用権IDを含むようにしても良く、この場合、コンテンツを指定すればそれを利用するために必要な利用権は一意に決まるため、両者のマッチングを決定する処理を行う必要はない。

【０１１７】

【発明の効果】本発明によれば、コンテンツを提供することができる。

【０１１８】また、本発明によれば、不正なコンテンツの利用を防止することができる。

【図面の簡単な説明】

【図１】従来のコンテンツの管理システムの模式図である。

【図２】本発明を適用したコンテンツ提供システムの構成例を示す図である。

【図３】図２のクライアントの構成例を示すブロック図である。

【図４】キーの構成を示す図である。

【図５】カテゴリノードを示す図である。

【図６】ノードとデバイスの対応例を示す図である。

【図７】有効化キーブロックの構成例を示す図である。

【図８】有効化キーブロックの他の構成例を示す図である。

【図９】有効化キーブロックの利用を模式的に表した図である。

【図１０】有効化キーブロックのフォーマットの例を示す図である。

【図１１】有効化キーブロックのタグの構成を説明する図である。

【図１２】本発明を適用したコンテンツの管理システムの模式図である。

【図１３】図１のクライアントのコンテンツ取り込み処理を説明するフローチャートである。

【図１４】コンテンツのフォーマットの例を示す図である。

【図１５】図１のクライアントの利用権生成処理を説明するフローチャートである。

【図１６】利用権のフォーマットの例を示す図である。

【図１７】図１のクライアントのコンテンツ再生処理を説明するフローチャートである。

【図１８】図１７のステップＳ４６における復号処理の詳細を説明するフローチャートである。

【図１９】図１８の復号処理を模式的に表した図である

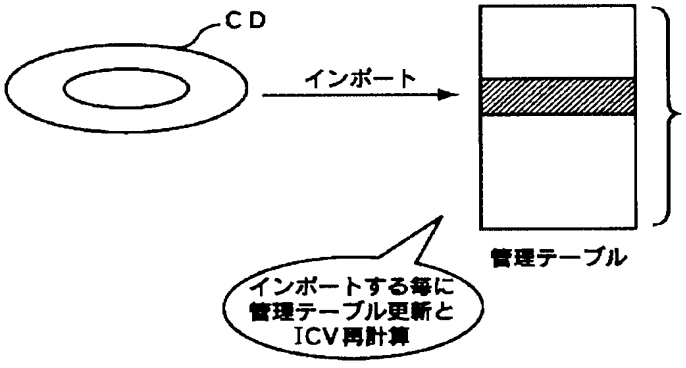
【図２０】図１９のEKBに含まれる情報の例を示す図である。

【符号の説明】

１－１，１－２　クライアント，　２　インターネット，　３　コンテンツサーバ，　４　ライセンスサーバ，　５　課金サーバ，　２０　タイマ，　２１CPU，　２４　暗号化復号部，　２５　コーデック部，　２６　入力部，　２７出力部，　２８　記憶部，　２９　通信部

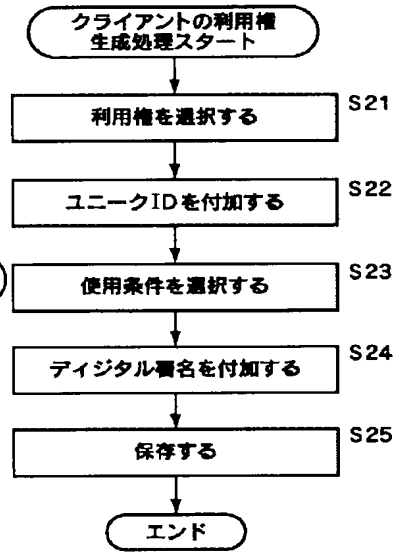
【図１】

図1



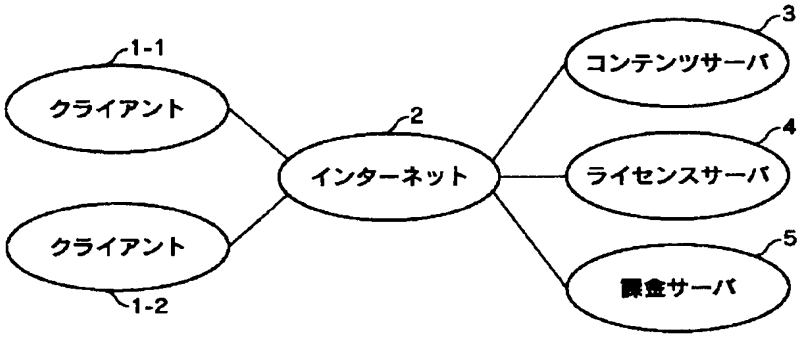
【図１５】

図15



【図２】

図2



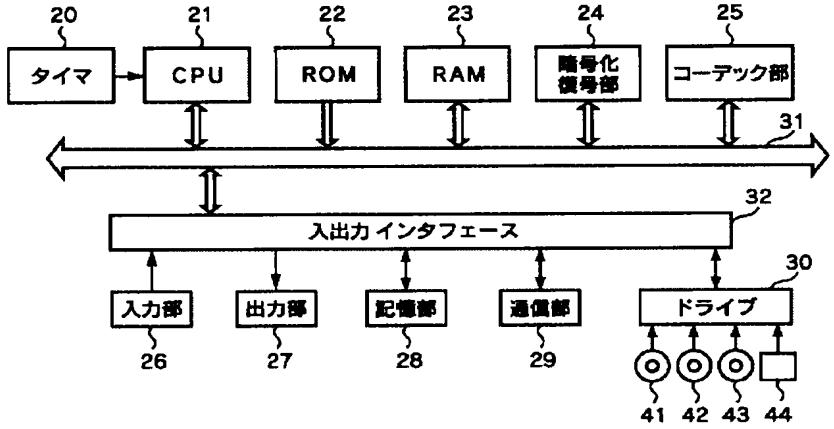
【図１６】

図16

バージョン
プロファイル
利用権ID
作成日時
有効期限
使用条件
コンテンツ条件
定数
ユニークID
署名
証明書

【図３】

図3



【図２０】

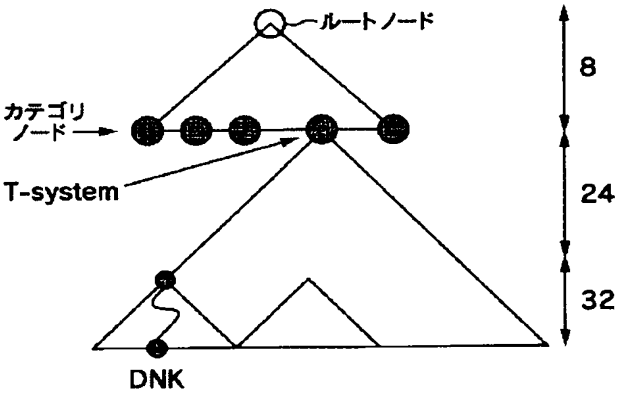
図20

EKB

Enc(DNK, Kroot)

【図５】

図5



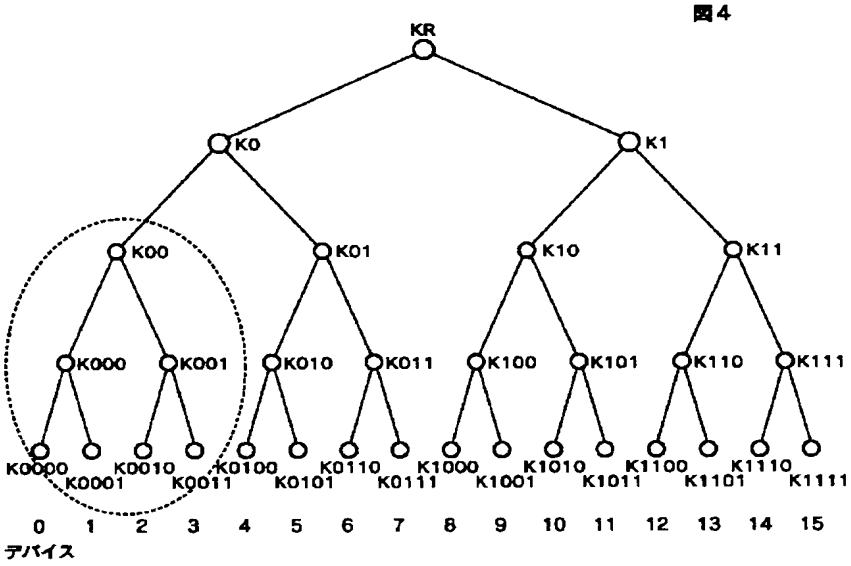
【図７】

図7

バージョン(Version) :t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

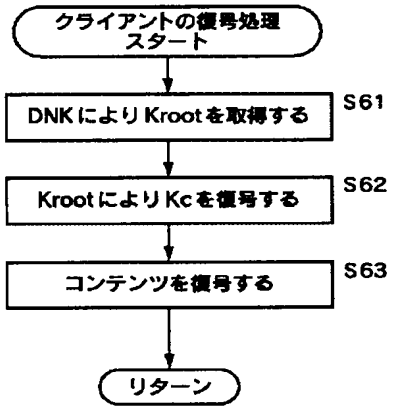
【図４】

図4



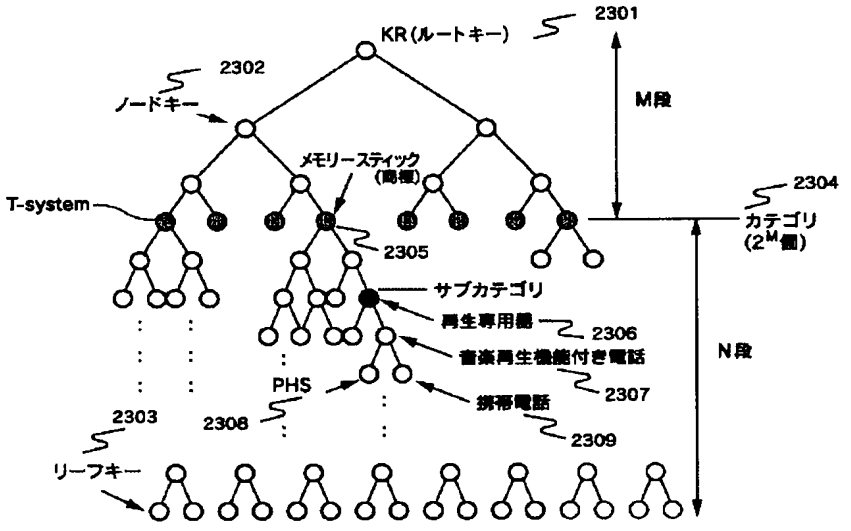
【図１８】

図18



【図６】

図6



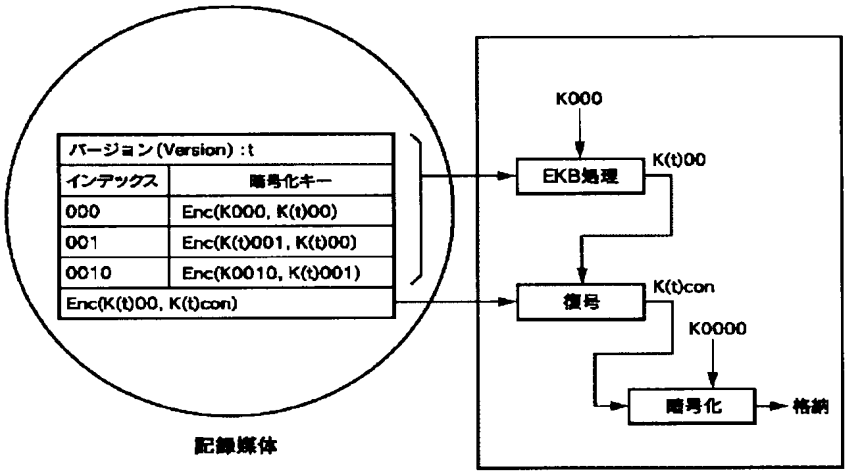
【図８】

図8

バージョン(Version) :t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

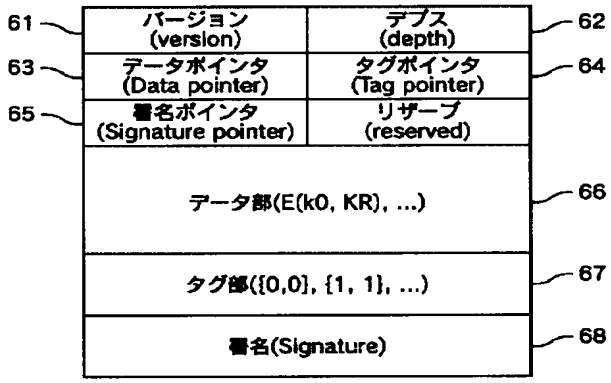
【図９】

図9



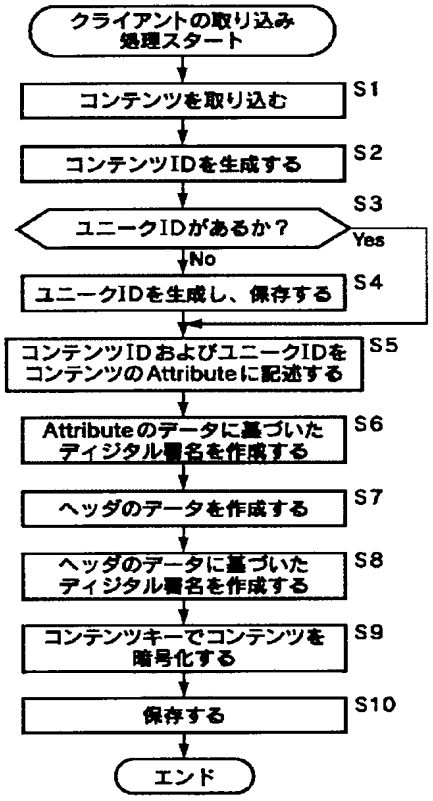
【図１０】

図10



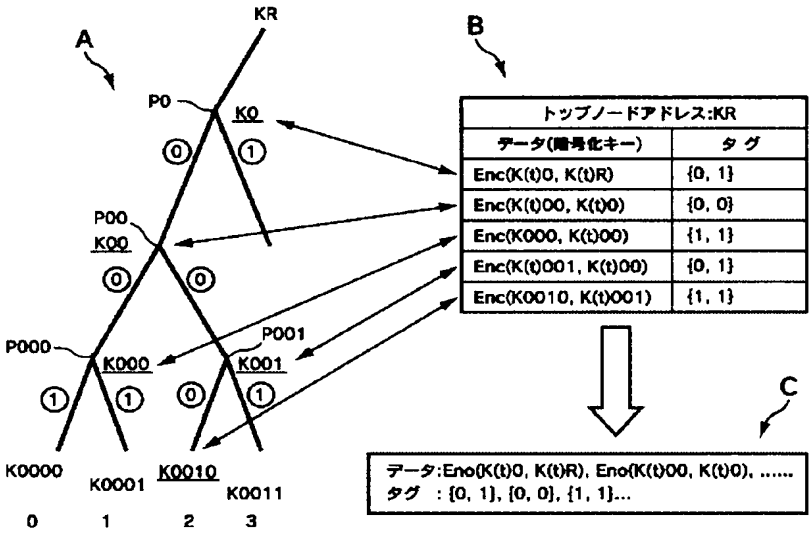
【図１３】

図13



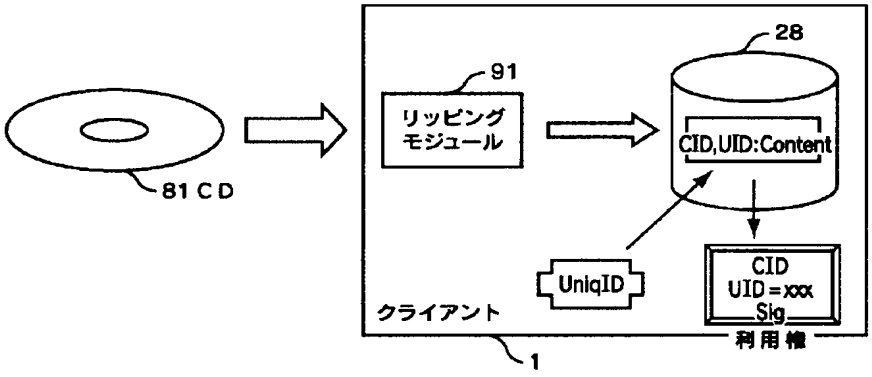
【図１１】

図11



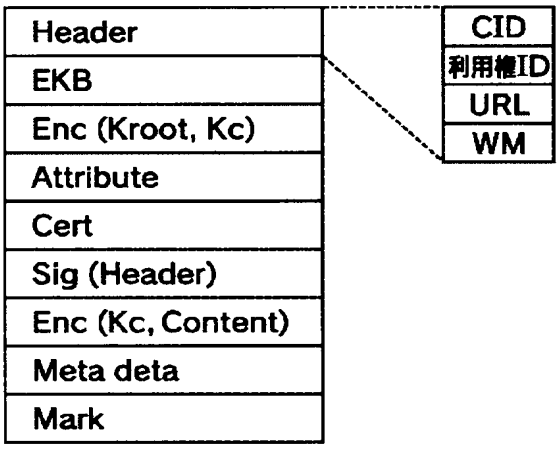
【図１２】

図12



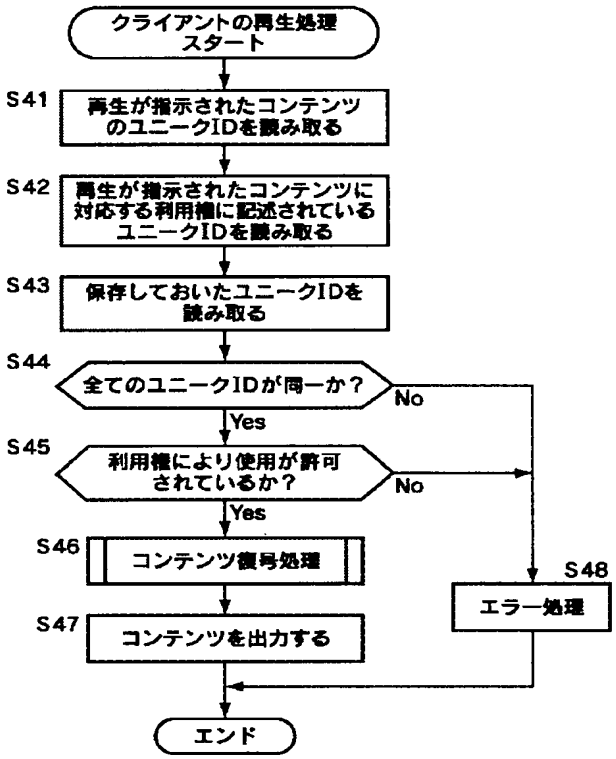
【図１４】

図14



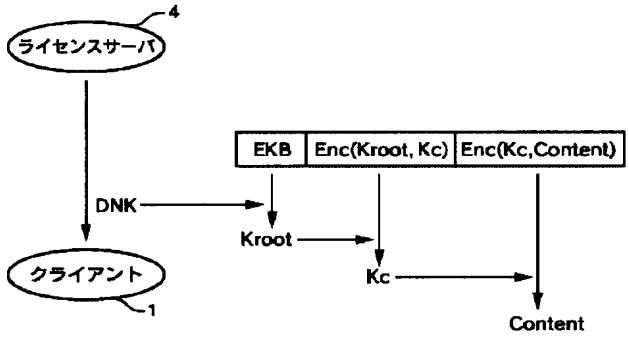
【図１７】

図17



【図１９】

図19



フロントページの続き

(72)発明者　江面　裕一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　長野　元彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考) 5B017 AA06 BB09 BB10 CA16
5B085 AE00 BA06 BG03 BG04 BG07
5C064 BA01 BB01 BB02 BC01 BC16
CB01 CC04
5D044 AB05 AB07 BC01 BC03 CC04
DE49 DE50 DE54 FG18 GK12
GK17 HH15 HL02 HL08 HL11